Abstract

In a method for protected execution of a cryptographic calculation in which a key (12) with at least two key parameters (p, q, pinv, sp, dp, sq, dq) is drawn on, an integrity check (30, 34, 40, 54) of the key (12) is performed, in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter (p, q, pinv, sp, dp, sq, dq) by corrupting at least one first key parameter (p, q, pinv, sp, dp, sq, dq). A further method serves to determine a key for a cryptographic calculation with at least two key parameters (p, q, pinv, sp, dp, sq, dq), provided for use in the first mentioned method. A computer program product and a portable data carrier have corresponding features. The invention enables particularly good protection of cryptographic calculations against attacks.

(Fig. 2)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
15. April 2004 (15.04.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/032411 A1

(51) Internationale Patentklassifikation[7]: H04L 9/30, 9/32, G06F 7/72

(21) Internationales Aktenzeichen: PCT/EP2003/010015

(22) Internationales Anmeldedatum: 9. September 2003 (09.09.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 42 061.0 11. September 2002 (11.09.2002) DE
102 50 810.0 31. Oktober 2002 (31.10.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

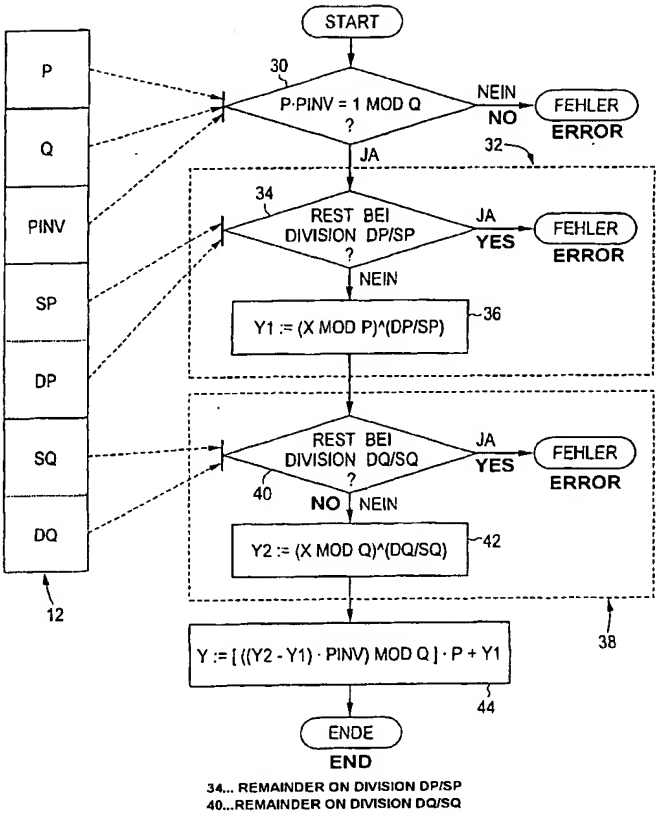
(75) Erfinder/Anmelder *(nur für US)*: **BOCKES, Markus** [DE/DE]; Spilhofstrasse 62, 81927 München (DE). **DREXLER, Hermann** [DE/DE]; Oberländerstrasse 5a, 81371 München (DE). **KAHL, Helmut** [DE/DE]; Zügelstrasse 9, 80992 München (DE).

(74) Anwalt: **DENDORFER, Claus**; Wächtershäuser & Hartz, Weinstrasse 8, 80333 München (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: PROTECTED CRYPTOGRAPHIC CALCULATION

(54) Bezeichnung: GESCHÜTZTE KRYPTOGRAPHISCHE BERECHNUNG



(57) Abstract: The invention relates to a method for carrying out a cryptographic calculation, whereby a key (12) with at least two key parameters (p, q, pinv, sp, dp, sq, dq) is used. An integrity check (30, 34, 40, 54) of the key (12) is carried out in order to prevent a cryptographic access, whereby conclusions about at least one second key parameter (p, q, pinv, sp, dp, sq, dq) can be drawn by means of falsifying at least one first key parameter (p, q, pinv, sp, dp, sq, dq). A further method serves for the determination of a key for a cryptographic calculation with at least two key parameters (p, q, pinv, sp, dp, sq, dq), provided for use in the first method. A computer programme product and a portable data support have corresponding features. The invention permits a particularly effective protection against attack for cryptographic calculations.

(57) Zusammenfassung: Bei einem Verfahren zum geschützten Ausführen einer kryptographischen Berechnung, bei der ein Schlüssel (12) mit mindestens zwei Schlüsselparametern (p, q, pinv, sp, dp, sq, dq) herangezogen wird, wird eine Integritätsüberprüfung (30, 34, 40, 54) des Schlüssels (12) durchgeführt, um einen kryptographischen Angriff zu verhindern, bei dem durch eine Verfälschung mindestens eines ersten Schlüsselparameters (p, q, pinv, sp, dp, sq, dq) Rückschlüsse auf mindestens einen zweiten Schlüsselparameter (p, q, pinv, sp, dp, sq, dq) gezogen werden. Ein weiteres Verfahren dient zum Bestimmen eines Schlüssels für eine kryptographische Berechnung mit mindestens zwei Schlüsselparametern (p, q, pinv, sp, dp, sq, dq), der zur Verwendung in dem erstgenannten Verfahren vorgesehen ist. Ein

Computerprogrammprodukt und ein tragbarer Datenträger

[Fortsetzung auf der nächsten Seite]

WO 2004/032411 A1